SECURITY PERFORMANCE ANALYSIS IN WIRELESS LANS

NURUL ANIS ANATI BINTI SARIPUDIN

Bachelor of Computer Science (Computer Systems & Networking)

UNIVERSITI MALAYSIA PAHANG

SUPERVISOR'S DECLARATION

I hereby declare that I have checked this thesis and in my opinion, this thesis is adequate in terms of scope and quality for the award of the degree of Bachelor of Computer Science (Computer Systems & Networking).

(Supervisor's Signature)

Full Name : Dr. Luhur Bayuaji

Position : Senior Lecturer

Date : 26 December 2018

STUDENT'S DECLARATION

I hereby declare that the work in this thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at Universiti Malaysia Pahang or any other institutions.

(Student's Signature)

Full Name : Nurul Anis Anati Binti Saripudin

ID Number : Ca15087

Date : 26 December 2018

SECURITY PERFORMANCE ANALYSIS IN WIRELESS LANS

NURUL ANIS ANATI BINTI SARIPUDIN

Thesis submitted in fulfillment of the requirements
for the award of the degree of
Bachelor of Computer Science (Computer Systems & Networking)

Faculty of Computer Systems & Software Engineering

UNIVERSITI MALAYSIA PAHANG

DECEMBER 2018

ACKNOWLEDGEMENTS

All praise to the Almighty ALLAH S.W.T for His blessing which has given me strength, patience and wisdom and ability during the final year project developing period. Sincere thanks to the God for giving me the opportunity to complete this project on time.

I would like to express my deepest appreciation to all those who provided me possibility to complete this project. A special gratitude to I give to my supervisor, Dr. Luhur Bayuaji for his insightful comments, outstanding advice and suggestions, spend time and helped me to coordinate my project especially in writing this thesis report.

Furthermore, I would like also to acknowledge with much thanks and appreciation to my friends for sharing their good idea and knowledge with me, in order to assist myself to succeed this project. I have to appreciate the guidance given by other supervisors as well as the panels and all lecturers throughout the completion of this project. Moreover, I am very grateful to both of my family for their love and endless support.

ABSTRAK

Protokol keselamatan telah dilaksanakan dalam rangkaian untuk memastikan bahawa data yang dihantar adalah dalam integriti dan keselamatan. Oleh itu, eksperimen ini adalah untuk menganalisis protokol keselamatan dalam prestasi WLAN berdasarkan piawaian IEEE 802.11 g / n. Eksperimen ini dijalankan menggunakan testbed untuk mengukur prestasi LAN tanpa wayar dari segi throughput dan purata tangguhan. Ia juga akan mengkaji interaksi antara lapisan keselamatan yang berlainan dan prestasi kesan mereka rangkaian sesak dan tanpa jujukan. Kajian ini juga akan menilai kesan UDP terhadap prestasi rangkaian di bawah protokol keselamatan yang berbeza.

ABSTRACT

The security protocol has been implemented within the network to ensure that the data sent is in integrity and security. Therefore, this experiment is to analyze the security protocol in performance of WLANs based on the IEEE 802.11 g/n standard. This experiment is conducted using a testbed to measure wireless LAN performance in terms of throughput, and average delay. It will also study the interaction between different security layers and their effect performance of congested and uncongested networks. This research will also evaluate the effect of UDP on the network performance under different security protocols.

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AES	Advanced Encryption Security
AP	Access Point
BSS	Basic Service Set
CBC-MAC	Cipher Block Chaining Message Authentication Code
CCMP	CBC-MAC Protocol
CMD	Command Prompt
CRC	Cyclic Redundance Unit
DSSS	Direct Sequence Spread Spectrum
ESS	Extended Service Set
ICV	Integrity Check Value
IV	Integrity Value
MIC	Michael or Message Integrity Code
MIMO	Multiple Input, Several Output
MPDU	MAC Protocol Data Unit
NR	Non-Roaming
OFDM	Orthogonal Frequency Division Multiplexing
RC4	Rivest Cipher 4
SDLC	System Development Life Cycle
SSID	Service Set Identifier
TKIP	Temporal Key Integrity
TP	Throughput
UDP	User Diagram Protocol
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WEP	Wired Equivalent Privacy

WLANs	Wireless Local Area Network

CHAPTER 1

INTRODUCTION

1.1 Background of Study

Wi-Fi abbreviated term for Wireless Fidelity which is general terms that referring to the IEEE 802.11 standard for Wireless Local Network or WLANs. WIFI is an alternative network for devices to connect in wireless mode rather than using the wired network. A local wireless network (WLAN) is a wireless distribution method for two or more devices using high- frequency radio waves, which often have an Internet access point. A WLAN enables users to move around the coverage area, often at home or in small office, while maintaining a network link. Sometimes a WLAN is called a local wireless network (LAWN). Development of WLAN standards based on the IEEE publication is 802.11a, 802.11b, 802.11g, and 802.11n where each standard has strengths and weaknesses in his application.

In WLANs around the world, security remained a major concern. Wireless networks offer comfort and flexibility, but they also increase network vulnerability. Security threats such as unauthorized access, denial of service attacks, spoofing of IP and MAC, hijacking and eavesdropping session can all be problems for WLANs. Various standard authentication and encryption techniques are combined with other access control mechanisms to address these threats. Collectively, these protocols, devices and techniques ensure the WLAN is equal to and even exceeds wired LAN security.

WEP (Wired Equivalent Privacy): An old standard for encryption used to overcome threats to security. WEP provides WLAN security by encrypting the information transmitted via the air so that only the receivers with the correct encryption key can decrypt the information. WPA (WI-FI Protected Access): Improved on the WEP by introducing Temporal Key Integrity Protocol (TKIP). While RC4 encryption is still

used, TKIP uses a temporal encryption key that is regularly renewed to make it harder to steal. Furthermore, the integrity of data has been improved through by using a more robust hashing mechanism. WPA2 (Wi-Fi Protected Access 2): improved on the WPA by introducing AES encryption algorithm. The AES is used in CBC-MAC Protocol (CCMP) to protect integrity and confidentiality in connection with AES key schedule. The CCMP use eight MIC bytes that are much stronger than Michael. Unlike WEP and TKIP, ICV is no longer needed.

The focus of the project is to examine the effect of security running on Wireless LANs. The project is test on the testbed in non-roaming network. Non-roaming network is access point (AP) and the clients are on the same network. While for roaming network, there are communication users in foreign networks for roaming network.

1.2 Problem Statement

Several security protocols and mechanisms to improve WLAN security are being developed. The implementations of security protocols therefore have an impact on network performance. However, there are no details on the extent to which degradation of network performance is affected by the security protocols in non-roaming networks.

Although the firmware of most wireless NICs can limit the interface for composing 802.11 standard packets, an attacker can still control any packet field using known techniques. It is therefore reasonable to assume that an attacker can generate any selected packet, modify packet's content, and fully control the packet's transmission.

At present, the wireless LAN system has a limited bandwidth, a longer response time and the wireless media is prone to error. This is caused by factors such as nature of the physical medium (air) itself, the number of users, the latency, the propagation factors like range and multipath. These can reduce LAN wireless performance.

1.3 Objective and Aim

The following are the objectives of this study to analyse the security performance in wireless LANs:

i. To compare the technique in Wi-Fi security protocol.

ii. To evaluate the effect of performance WLAN (IEEE 802.11g/n) for various security protocols

iii. To identify the effect of uncongested and congested network on UDP traffic stream.

1.4 Scope

The scope for the research is for the user that uses the wireless LANs to communicate with each other. The user who acts as a sender must be in one network to be able to send the data that they want to the receiver. The access point has the built-in DHCP server. It will assign the IP address to the devices that connect to the Wi-Fi.

The packet that sends from sender to receiver is capture by the Wireshark. The sender will generate the packet using TFGEN. This testbed is implemented in Windows 10.

1.5 Significance

The important of this analysis is to ensure your system meets security and performance requirements by conduct wireless LAN (WLAN) testing. Next, it can help the designers to choose which security protocol can be implemented in a given network scenario.

1.6 Thesis organization

Chapter 1 consists of the project introduction, which is the general introduction. Then the related problem statement continued. The objectives of the project are also clearly stated in conjunction with the aim. Finally, the project's scope to show the related field according to project title.

Chapter 2 is the review of the project literature. In this chapter, information on the research study in general is described.

REFERENCES

Jindal, Poonam, and Brahmjit Singh. 2017. "Quantitative Analysis of the Security Performance in Wireless LANs." *Journal of King Saud University - Computer and Information Sciences* 29(3): 246–68. http://dx.doi.org/10.1016/j.jksuci.2014.12.012.

Local, On Wireless. 2006. "Security Impacts Networks." : 123–27.

Baghaei, N, and R Hunt. 2004. "IEEE 802.11 Wireless LAN Security Performance Using Multiple Clients." *Proceedings 2004 12th IEEE International Conference on Networks ICON 2004 IEEE Cat No04EX955* 1: 299–303. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1409151.

Butty, Levente. "WiFi Security : WEP and Its Flaws Why Security Is More of a Concern in Wireless ? Introduction to WiFi."

Cam-winget, By Nancy, Russ Housley, David Wagner, and Jesse Walker. "No Title." 46(5): 35–39.

Government, The, Hong Kong, Special Administrative, and Region The. 2010. "Wireless Networking Security."

Potlapally, N. R., S. Ravi, A. Raghunathan, and N. K. Jha. 2006. "A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols." *IEEE Transactions on Mobile Computing* 5(2): 128–43.

Sheldon, Frederick T., John Mark Weber, Seong Moo Yoo, and W. David Pan. 2012. "The Insecurity of Wireless Networks." *IEEE Security and Privacy* 10(4): 54–61.